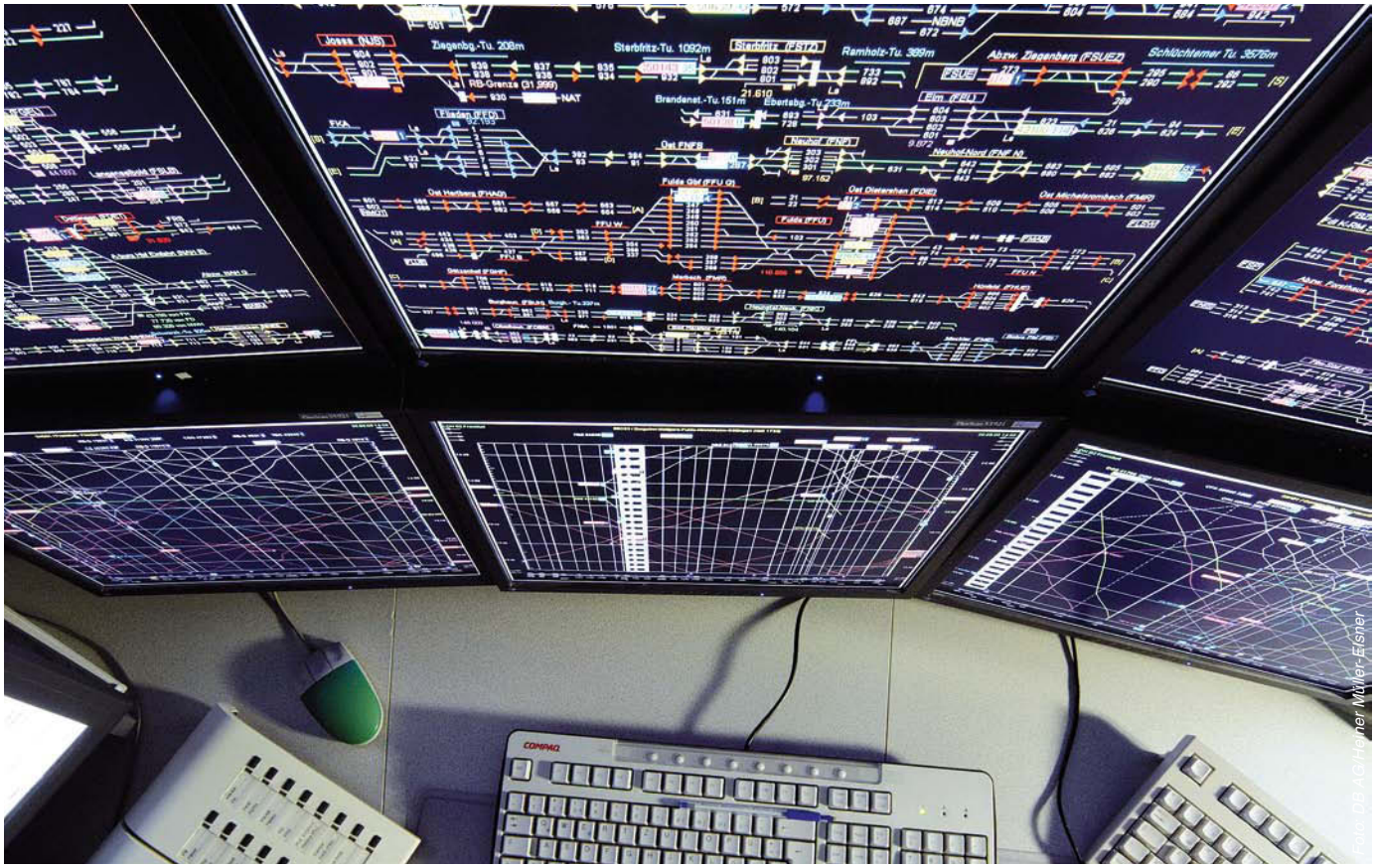

Foto: DB AG/Heiner Müller-Elsner

Common Safety Methods

Grundbegriffe für Sicherheits- und Risikobetrachtungen

Dr.-Ing. Gunnar Bosse, Institut für Eisenbahnwesen und Verkehrssicherung der Technischen Universität Braunschweig

Die Begrifflichkeiten von Sicherheits- und Risikoanalysen gewinnen im Rahmen der Sicherheitsarbeit der Eisenbahnen immer weiter an Bedeutung. Mit diesem Beitrag soll ein Brückenschlag zwischen wissenschaftlicher Modellbildung und praktischer Anwendung geleistet werden. Es werden elementare Begriffe in möglichst anschaulicher Weise erklärt und die zwischen ihnen bestehenden Zusammenhänge erläutert.

https://doi.org/10.24355/dbbs.084-202005050938-0

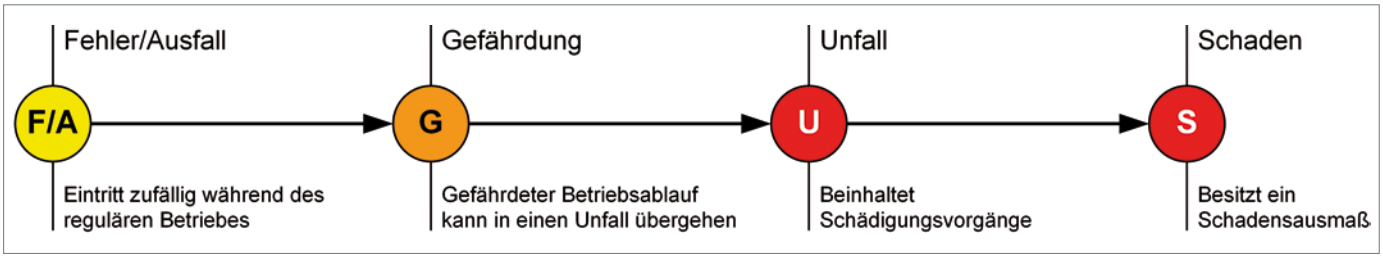

Abbildung 1: Die Wirkungskette vom Fehler/Ausfall zum Schaden

Der Beitrag baut zum einen auf der wissenschaftlichen Arbeit des Autors auf diesem Gebiet auf[1)] und berücksichtigt zum anderen Erfahrungen, die er unter anderem in Seminaren sammeln konnte, welche er im Auftrag von DB Training als Trainer durchgeführt hat. Er folgt dabei dem Motto „so viel Wissenschaftlichkeit wie nötig, so viel Anschaulichkeit wie möglich".

Sicherheits- und Risikoanalysen sind seit langem ein fester Bestandteil der Sicherheitsarbeit im Eisenbahnwesen und ein Teil der Entwicklungs- und Zulassungsprozesse neuer Systeme. Mit der europäischen Verordnung 352/2009 „über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken"[2)] wird den Eisenbahnunternehmen nun auch ein Rahmen für den Umgang mit Änderungen am bestehenden Eisenbahnsystem vorgeben.

Diese auch als CSM-RA (Common Safety Method for Risk Assessment) bezeichnete Verordnung konkretisiert die Europäische Sicherheitsrichtlinie[3)] und ist seit dem 1. Juli 2012 von den Eisenbahnunternehmen bei der Änderung von Systemen und auch Prozessen anzuwenden. Damit vergrößert sich der Kreis von Personen, die sich mit den entsprechenden Begrifflichkeiten und Verfahrensschritten auseinanderzusetzen haben. In den Eisenbahnunternehmen sind insbesondere diejenigen Personen, die eine Änderung am bestehenden und damit zugelassenen Eisenbahnsystem vornehmen möchten, als Vorschlagende für die Umsetzung und Einhaltung einer verordnungskonformen Vorgehensweise verantwortlich.

In der Verordnung werden die Vorgehensweisen nicht näher vorgegeben. Dies bleibt Aufgabe der einzelnen Eisenbahnunternehmen. Sie begleiten die Einführung der Vorgehensweisen unter anderem mit Schulungsmaßnahmen, zum Beispiel in Zusammenarbeit mit DB Training, aber auch mit unternehmensbereichsspezifischen Leitfäden und anderen Dokumenten, die auch auf Gruppenlaufwerken bereitgestellt werden. Darüber hinaus stellen auch die Aufsichtsbehörden Leitfäden zur Verfügung, wie zum Beispiel das Eisenbahn-Bundesamt[4)].

Es liegt auf der Hand, dass ein einzelner Beitrag hier weder den Stand der sich entwickelnden Vorgehensweisen noch die entsprechenden Prozessabläufe vollumfänglich wiedergeben kann. Dieser Beitrag beschränkt sich daher auf eine mit Beispielen ergänzte Erläuterung der im CSM-RA-Prozess immer wiederkehrenden Begriffe der Risikoanalyse.

Risiko

Wie sich aus dem Namen der Verordnung bereits ergibt, handelt es sich bei der anzuwendenden Vorgehensweise um einen risikobasierten Ansatz. Es scheint daher sinnvoll, sich zunächst dem Begriff „Risiko" und damit verbundenen weiteren Begriffen und Wirkungszusammenhängen zu nähern.

Der Begriff „Risiko" ist im Prinzip allgegenwärtig. Jeder verwendet ihn. „No risk – no fun" und „Wer nicht wagt, der nicht gewinnt" sind nur zwei Beispiele, mit denen häufig zum Ausdruck gebracht wird, dass eine Unternehmung oder ein Vorhaben auch einmal schief gehen und zu einem ungewollten Ereignis, möglicherweise verbunden mit einem Schaden, führen kann. Auch in der Feststellung „Nichts ist zu 100 Prozent sicher" kommt diese lebensnahe Erkenntnis zum Ausdruck. Wir leben in einer Welt voller Risiken und sind gezwungen, sie einerseits ein Stück weit zu akzeptieren, andererseits aber auch zu steuern.

„Das war aber knapp!", „Das ist gerade noch einmal gutgegangen!" oder „Das war aber gefährlich!" sind Umschreibungen für Situationen, aus denen sich ein Unfall hätte ergeben können. Ein riskantes Überholmanöver im Straßenverkehr oder auch ein geplatzter Autoreifen sind Beispiele für gefährliche Situationen, die beim Betrieb von Kraftfahrzeugen auftreten können. Sie sind Gefährdungen des Betriebs.

Die Ursachen dieser Gefährdungen können menschliche Fehlhandlungen, zum Beispiel ein riskantes Überholmanöver, oder technische Ausfälle sein, zum Beispiel das Platzen eines Reifens bzw. Fehler bei der Bemessung, Konzeption oder der Fertigung des Reifens. Sie werden im Folgenden als Fehler und Ausfälle zusammengefasst.

Der Begriff Risiko basiert folglich auf einer qualitativen, von Fehlern oder Ausfällen ausgehenden, über die Gefährdung und den Unfalleintritt bis hin zu einem Schaden reichenden Wirkungskette. Diese beginnt mit Fehlern und Ausfällen, die im bis dahin regulär ablaufenden Betrieb auftreten, und eskaliert in mehreren Stufen bis hin zu einem Schaden (Abbildung 1).

Werden die Bestandteile der Risiko-Wirkungskette quantifiziert, das heißt mit Zahlen hinterlegt, wird Risiko messbar und Sicherheit bewertbar. Wie wahrscheinlich ist ein Unfall? Wie groß sind die zu erwartenden Schäden? Letztlich lässt sich Risiko mittels folgender drei Faktoren messen und bewerten:

Gefährdungswahrscheinlichkeit

Aus den Fehler- und Ausfallraten der Komponenten eines Systems kann beispielsweise ermittelt werden, wie groß die Wahrscheinlichkeit für das Eintreten eines gefährlichen Zustandes (Gefährdung) sein wird. Die Raten werden dazu in Fehlerbäumen entsprechend der Architektur des Systems miteinander verknüpft.

https://doi.org/10.24355/dbbs.084-202005050938-0

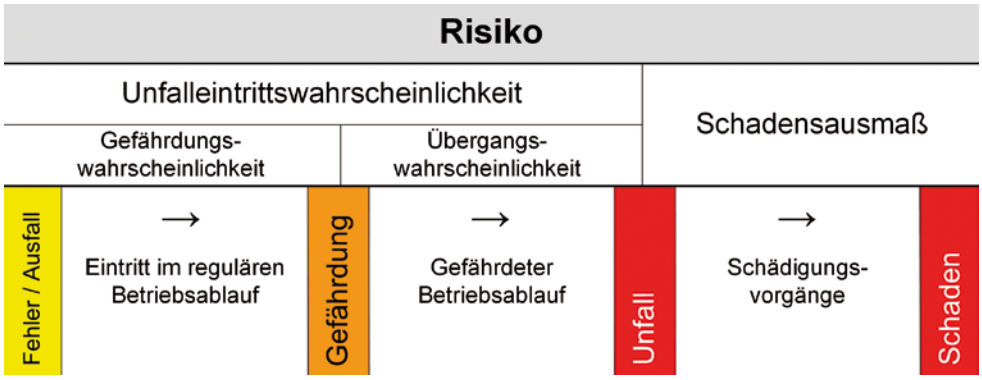

Abbildung 2:
Die Faktoren und Zusammenhänge der Risikoformel

Alle Grafiken Quelle: Gunnar Bosse

Übergangswahrscheinlichkeit (zu einem Unfall)

Der zweite Faktor beschreibt, wie häufig eine eingetretene Gefährdung in einen Unfall übergeht. Damit wird berücksichtigt, dass nicht jede Gefährdung automatisch in einen Unfall mündet, da Unfälle häufig „nur" die Spitze eines Eisberges sind. Die Übergangswahrscheinlichkeiten können auf der Basis (statistisch festgehaltener) Erfahrungen ermittelt werden und/oder, wenn dies nicht möglich ist, auch auf Expertenschätzungen beruhen.

Schadensausmaß

Als dritter Faktor wird das Schadensausmaß in die Risikoformel einbezogen. Mit ihm wird der bei einem Unfalleintritt zu erwartende Schaden quantifiziert. Hierbei spielen unter anderem die betrieblichen Gegebenheiten, wie zum Beispiel die Geschwindigkeit, unter denen der Unfall eintritt, eine große Rolle. Auch das Schadensausmaß kann auf Basis statistischer Auswertungen oder mittels Expertenschätzungen bestimmt werden.

Das von einem betrachteten System ausgehende Risiko wird folglich als Produkt aus Gefährdungswahrscheinlichkeit, Übergangswahrscheinlichkeit zu einem Unfall und dem damit verbundenen Schadensausmaß berechnet (Abbildung 2).

Risiko-Stellschrauben

Um das von einem System ausgehende Risiko zu beherrschen, das heißt auf ein akzeptiertes und damit zulässiges Maß zu senken, ergeben sich ausgehend von der Risikoformel drei prinzipielle Ansatzpunkte: das Beherrschen der Gefährdungen, das Beeinflussen der Wahrscheinlichkeit für einen Übergang von einer eingetretenen Gefährdung zu einem Unfall sowie das Eingrenzen des Schadensausmaßes im Falle eines Unfalls.

Grundsätzlich machen alle Verkehrssysteme, egal ob die Eisenbahn, die Luftfahrt oder der Straßenverkehr von diesen Möglichkeiten Gebrauch; dies jedoch ihren Sicherheitsphilosophien entsprechend mit zum Teil sehr unterschiedlichen Schwerpunkten.

Während im Eisenbahnwesen das Vermeiden gefährlicher Situationen im Vordergrund steht und die passive Sicherheit eine eher untergeordnete Rolle spielt, haben im Straßenverkehr insbesondere passive Sicherheitsmaßnahmen zu einer deutlichen Reduzierung des Risikos beigetragen. Neuerdings sind aber auch hier neuere Systeme im Kommen, die in gefährlichen Situationen eingreifen, um einen Unfall abzuwenden.

Beherrschen der Gefährdung

Ideal wäre es natürlich, wenn die für den Betrieb eines Verkehrssystems erforderlichen Funktionen bei ihrer Ausführung möglichst nicht versagen. Dies würde nicht nur eine hohe Verfügbarkeit gewährleisten, sondern auch einen guten Schutz vor dem Eintreten von Gefährdungen bieten. Ist dieser Schutz vorhanden, wird von einer „Beherrschung der Gefährdung" gesprochen. Da es keine hundertprozentige Sicherheit geben kann, gilt eine Gefährdung als beherrscht, wenn sie nicht häufiger als nach dem akzeptierten Risiko zulässig eintritt.

Die Maßnahmen zur Beherrschung von Gefährdungen sind dadurch charakterisiert, dass sie – zeitlich betrachtet – wirken sollen, bevor die zu beherrschende Gefährdung eintreten kann. Anders ausgedrückt: Das Versagen einer Maßnahme zur Beherrschung einer Gefährdung würde mit zum Entstehen der entsprechenden Gefährdung beitragen. Sie liegt folglich in der Wirkungskette vor der betrachteten Gefährdung.

Zu den Maßnahmen zur Beherrschung der Gefährdung gehören Maßnahmen, die das Auftreten von Fehlern und Ausfällen verhindern. Ferner gehören dazu auch Maßnahmen, die das Eintreten von Fehlern und Ausfällen so frühzeitig aufdecken, dass das Eintreten einer Gefährdung abgewendet werden kann, indem das System rechtzeitig in einen sicheren Zustand, zum Beispiel den Haltzustand überführt wird (Fail-Safe-Prinzip). Dies kann zum Beispiel durch den Einsatz von Mehrrechnersystemen erfolgen, die übereinstimmende Ergebnisse liefern müssen, bevor ein nächster Prozessschritt ablaufen darf.

Abwehren eines Unfalleintritts

Das Eintreten einer Gefährdung ist nicht gleichbedeutend mit dem Eintritt eines Unfalls. In der Regel tragen von den örtlichen Situationen und betrieblichen Faktoren abhängige Ereignisabläufe dazu bei, dass nicht aus jeder Gefährdung ein Unfall entsteht. Öffnet sich beispielsweise ein bereits geschlossener Bahnübergang vorzeitig, so muss es nicht zwangsläufig zu einem Unfall kommen. Durch glückliche Umstände, die den Charakter des Zufälligen haben, kann die Gefährdung auch glimpflich ausgehen.

https://doi.org/10.24355/dbbs.084-202005050938-0

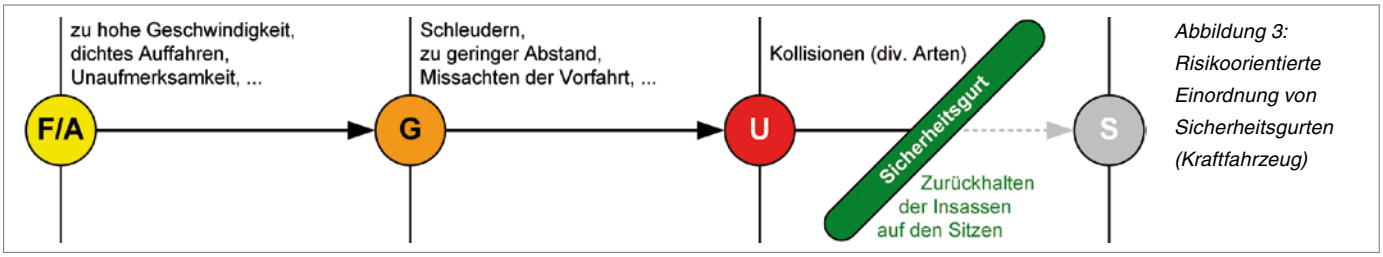

Abbildung 3: Risikoorientierte Einordnung von Sicherheitsgurten (Kraftfahrzeug)

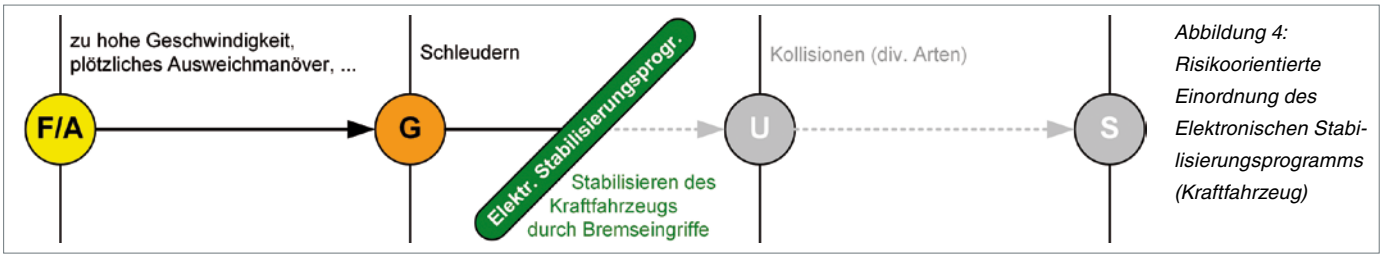

Abbildung 4: Risikoorientierte Einordnung des Elektronischen Stabilisierungsprogramms (Kraftfahrzeug)

Die Wahrscheinlichkeit für den Übergang von einer bereits eingetretenen Gefährdung zu einem Unfall kann aber auch durch gezielte Maßnahmen beeinflusst werden. Auch die Eisenbahn kennt solche ergänzenden Maßnahmen. Der Durchrutschweg hat beispielsweise keine betriebliche Funktion, denn er wird für eine Fahrt von A nach B nicht benötigt. Im Gegenteil, er verlängert unter Umständen die Gleisanlagen bzw. sorgt für zusätzliche Fahrstraßenausschlüsse. Andere Eisenbahnen, wie zum Beispiel die Österreichischen Bundesbahnen, kommen ohne ihn bzw. mit kürzeren Längen aus. Der Durchrutschweg wird allein für den Fall vorgehalten, dass beispielsweise beim bereits als Gefährdung anzusehenden Verbremsen die Wahrscheinlichkeit für eine Kollision mit einem anderen Zug reduziert wird, indem eine zusätzliche Bremsstrecke von anderen Zügen freigehalten wird.

Die Maßnahmen zur Abwehr eines Unfalleintritts sind also dadurch geprägt, dass sie zum Erfüllen der eigentlichen Betriebsaufgabe nicht benötigt werden. Sie entfalten ihre Wirkung erst nach dem Eintritt einer Gefährdung, indem sie in die nach dem Gefährdungseintritt ablaufenden Ereignisabläufe eingreifen und damit die Übergangswahrscheinlichkeit zu einem Unfall senken.

Begrenzen des Schadensausmaßes

Lässt sich der Eintritt eines Unfalls nicht verhindern, kann das bestehende Risiko durch Maßnahmen reduziert werden, die das Schadensausmaß senken. Diese auch als passive Sicherheit bezeichneten Maßnahmen stehen im Eisenbahnwesen wegen der starken Orientierung auf aktive Sicherheitsmaßnahmen zur Beherrschung der Gefährdungen nicht so sehr im Vordergrund. Im Bereich des Straßenverkehrs sind sie dagegen weit verbreitet. Als Beispiele seien dort Knautschzonen sowie Sicherheitsgurte und Airbags genannt.

Beispiele für Maßnahmen zur Reduzierung des Risikos und ihre Einordnung

Jede geplante oder auch bereits existierende Maßnahme zur Beeinflussung des Risikos kann einem der drei vorstehend erläuterten Prinzipien zugeordnet werden. Dies kann mit Hilfe der Wirkungskette und der Einordnung vor oder nach Gefährdungseintritt oder Unfalleintritt vorgenommen werden. Für die Einordnung einer Maßnahme ist allerdings nicht entscheidend, wann sie durchgeführt oder vorbereitet wird, sondern ausschließlich wann sie ihre Wirkung entfalten soll. Dies wird nachfolgend anhand einiger Beispiele aus dem Bereich des Straßenverkehrs und der Eisenbahn erläutert:

Sicherheitsgurte

In Kraftfahrzeugen sind Sicherheitsgurte bereits zu Fahrtbeginn und damit vor dem Eintritt einer Gefährdung anzulegen. Ihre Wirkung entfalten sie jedoch erst nach dem Eintritt eines Unfalls, in dem sie die Fahrzeuginsassen bei der Kollision im Sitz zurückhalten. Sie ist deshalb den Maßnahmen zur Reduzierung des Schadensausmaßes zuzurechnen (Abbildung 3).

Elektronisches Stabilisierungsprogramm

Elektronische Stabilisierungsprogramme (ESP) finden seit mehreren Jahren eine immer größere Verbreitung in Kraftfahrzeugen. Ein ESP greift in kritischen Fahrsituationen, zum Beispiel beim Ausbrechen des Kraftfahrzeugs durch gezieltes Ansteuern der Bremsen ein, um das Fahrzeug in seinem Fahrverhalten zu stabilisieren und steuerbar zu halten. Fahrfehler, die zu den kritischen Situationen führen, werden durch das System nicht vermieden. Es sollen vorrangig Kollisionen unter anderem mit anderen Kraftfahrzeugen oder Bäumen vermieden werden. Im Gegensatz zum Sicherheitsgurt liegt die Wirkung des ESP bereits vor einem potenziellen Unfall, das bedeutet, es ist den Maßnahmen zur Abwehr eines Unfalleintritts zuzuordnen (Abbildung 4).

Durchrutschweg

Im Eisenbahnwesen wird ein Durchrutschweg als Teil der Fahrstraße vor der Zulassung einer Fahrt eingestellt, bereitgehalten und überwacht. Er entfaltet seine Wirkung jedoch erst mit seiner Inanspruchnahme nach dem Eintreten einer potenziell gefährlichen Situation, zum Beispiel beim Verbremsen. Er wirkt aber bereits vor dem Eintritt eines Unfalls. Er gehört somit den Maßnahmen zur Abwehr eines Unfalleintritts und senkt die Übergangswahrscheinlichkeit (Abbildung 5).

https://doi.org/10.24355/dbbs.084-202005050938-0

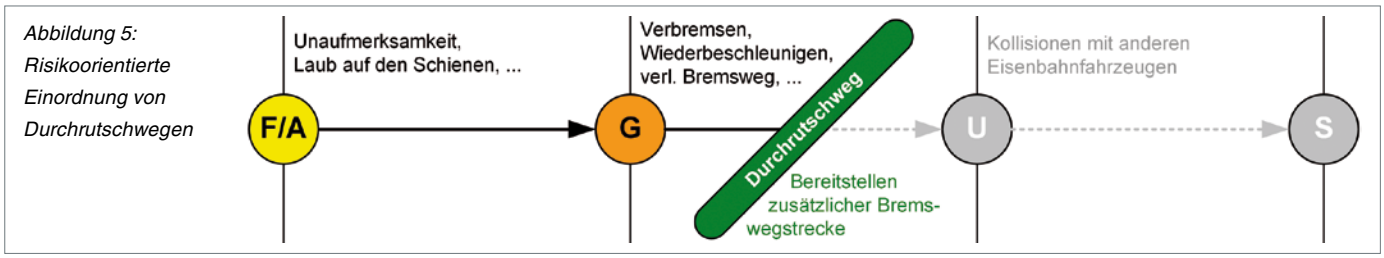

Abbildung 5: Risikoorientierte Einordnung von Durchrutschwegen

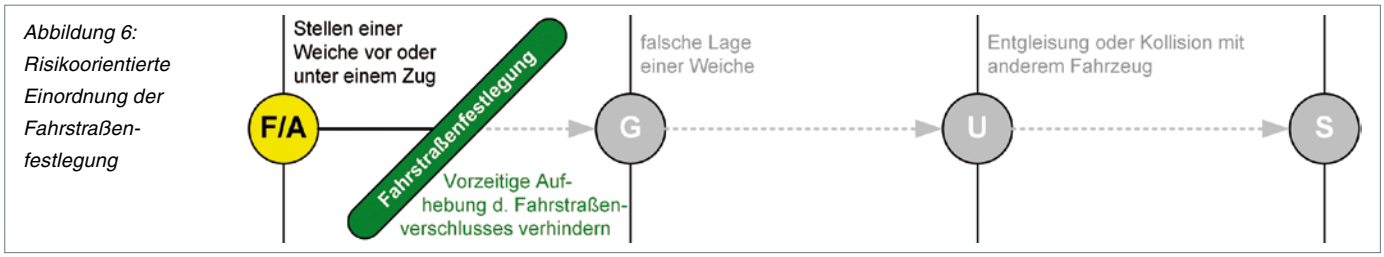

Abbildung 6: Risikoorientierte Einordnung der Fahrstraßen-festlegung

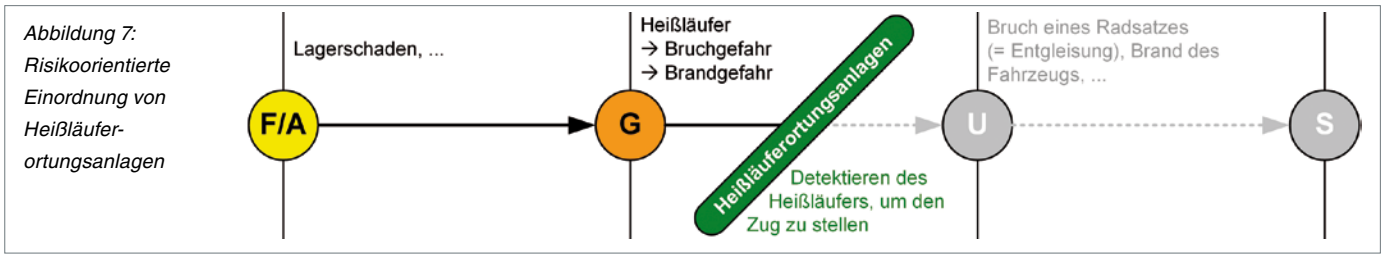

Abbildung 7: Risikoorientierte Einordnung von Heißläufer-ortungsanlagen

Fahrstraßenfestlegung

In Stellwerken wird mit der Festlegung von Fahrstraßen verhindert, dass fehlerhafterweise ein Fahrstraßenverschluss zurückgenommen wird, bevor ein Zug die Fahrstraßenzugschlussstelle freigefahren hat oder am vorgeschriebenen Halteplatz zum Halten gekommen ist. Mit der Festlegung wird einer Gefährdung entgegengewirkt, bei der beispielsweise eine für die freigegebene Fahrstraße eingestellte Weiche in eine andere Lage gestellt wird, bevor der Zug sie befahren hat. Die Fahrstraßenfestlegung ist somit eine Maßnahme zur Beherrschung einer Gefährdung (Abbildung 6).

Heißläuferortungsanlage

Eine Heißläuferortungsanlage (HOA) dient dem Detektieren von Radsätzen, deren Betriebstemperatur auffällig nach oben abweicht. Ziel ist das rechtzeitige Stellen des entsprechenden Zuges, bevor es zum Beispiel durch den Bruch des Radsatzes oder das Entstehen eines Brandes zu einem Unfall kommen kann. Eine HOA wirkt folglich vor einem potenziellen Unfall. Sie kann das Entstehen erhöhter Betriebstemperaturen jedoch nicht verhindern. Sie wirkt folglich erst nach dem Eintreten eines Zustandes, der wegen einer möglichen Unfallfolge als gefährlich einzustufen ist. Eine HOA ist deshalb den Maßnahmen zur Abwehr eines Unfalleintritts zuzuschreiben (Abbildung 7).

Entgleisungsdetektoren

Im Eisenbahnwesen nicht verbreitete, aber vorstellbare Entgleisungsdetektoren würden die Radsätze oder Drehgestelle von Zügen bereits während der Fahrt überwachen. Ihre Wirkung würde jedoch erst nach dem Entgleisen eintreten. Da mit einer Entgleisung bereits ein Unfall vorliegt, wären Entgleisungsdetektoren den Maßnahmen zur Reduzierung des Schadensausmaßes zuzuordnen (Abbildung 8).

Mündliche Wiederholungen

Im Rahmen eines Zugmeldeverfahrens sind zum Beispiel für das Anbieten, Annehmen, Abmelden und Rückmelden nicht nur exakte Wortlaute, sondern auch mündliche Wiederholungen durch den jeweils anderen Fahrdienstleiter vorgeschrieben, um Missverständnisse zu vermeiden, die zu gefährlichen Situationen führen können. Die mündlichen Wiederholungen sind folglich Maßnahmen, die der Beherrschung einer Gefährdung dienen (Abbildung 9).

Zugbeeinflussungssysteme

Mit Hilfe von Zugbeeinflussungssystemen werden Daten über die zulässige Fahrweise vom Fahrweg zum Fahrzeug übertragen, um dort beim Abweichen von der erlaubten Fahrweise Schutzreaktionen (Zwangsbremsungen) auszulösen[5] Angesichts mittlerweile sehr ausgefeilter punkt- und linienförmiger Beeinflussungssysteme, welche die Triebfahrzeugführer bereits nah an der erlaubten Fahrweise überwachen und gegebenenfalls eingreifen, stellt sich die Frage, ob diese Systeme der Abwehr eines Unfalls nach einer bereits eingetretenen gefährlichen Situation dienen oder bereits den Maßnahmen zur Beherrschung einer Gefährdung zuzurechnen sind. Dies ist letztlich eine Frage der Definition ihrer Aufgabe. Es ist unstrittig, dass das Abweichen von der erlaubten Fahrweise eine nicht beabsichtigte Situation ist und dass sich aus ihr ein Unfall entwickeln kann. Deshalb sind Abweichungen von der erlaubten Fahrweise als

https://doi.org/10.24355/dbbs.084-202005050938-0

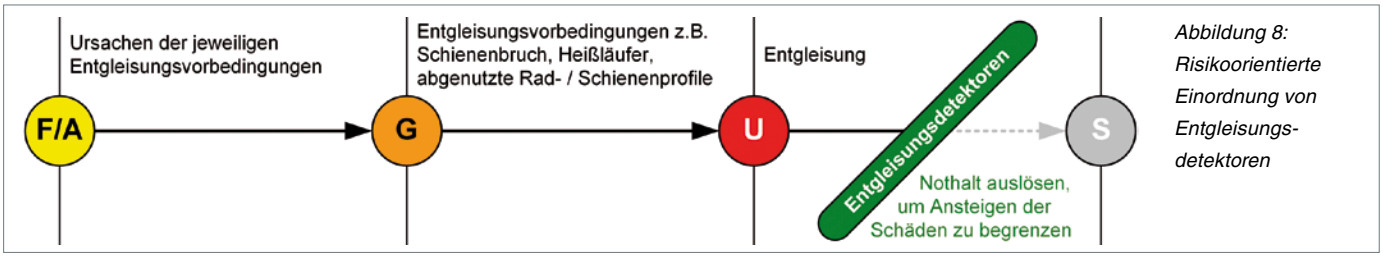

Abbildung 8: Risikoorientierte Einordnung von Entgleisungsdetektoren

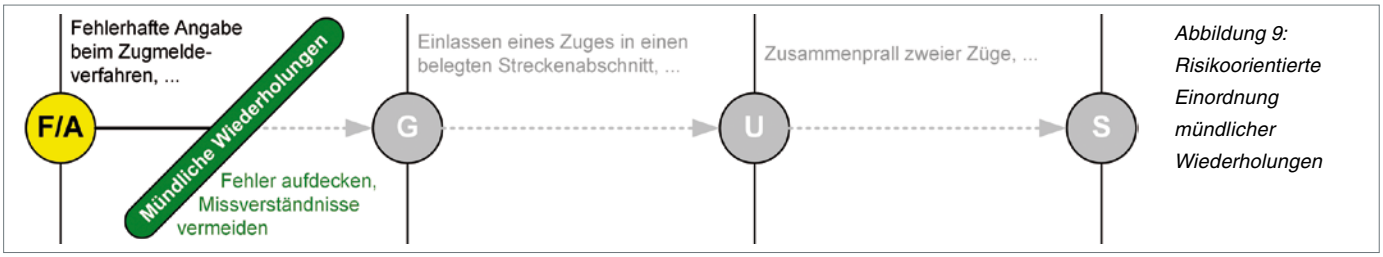

Abbildung 9: Risikoorientierte Einordnung mündlicher Wiederholungen

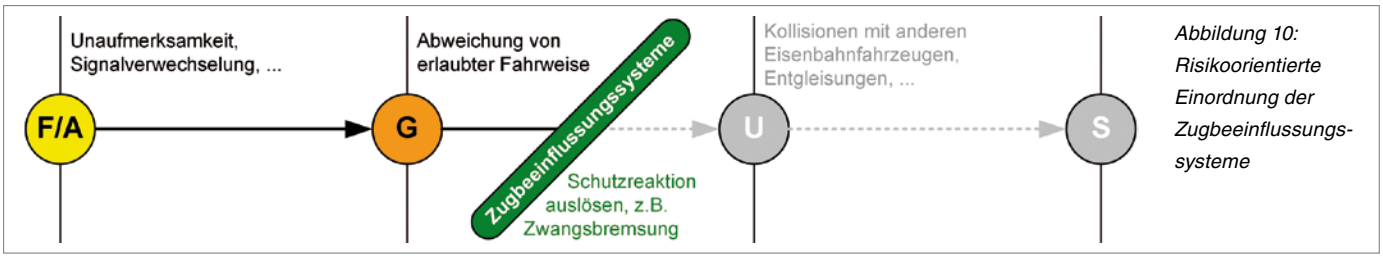

Abbildung 10: Risikoorientierte Einordnung der Zugbeeinflussungssysteme

Gefährdungen einzustufen. Sollen die Zugbeeinflussungssysteme beim Abweichen von der erlaubten Fahrweise wirken, dann ist die potenziell gefährliche Situation bereits eingetreten, und es geht um die Abwehr eines möglichen Unfalls. Sollen die Zugbeeinflussungssysteme dagegen das Abweichen von der erlaubten Fahrweise von vornherein verhindern, dann wären sie den Maßnahmen zur Beherrschung einer Gefährdung zuzurechnen. Da entwicklungsgeschichtlich und auch rechtlich die Verantwortung für die Fahrweise eines Zuges weiterhin dem Triebfahrzeugführer obliegt und die Zugbeeinflussungssysteme erst bei Abweichungen davon eingreifen, sind die klassischen Systeme als Maßnahmen zur Abwehr eines Unfalls einzustufen, auch wenn sie zum Teil bereits automatische Fahrweisen erlauben. Hingegen sollten Zugbeeinflussungssystemen, welche die Aufgabe haben, die Fahrweise eines Zuges nicht nur zu überwachen, sondern vordergründig den Zug zu steuern, wie zum Beispiel bei vollautomatischen fahrerlosen Bahnen, den Maßnahmen zur Beherrschung der Gefährdung zugeordnet werden (Abbildung 10).

Gefährdung

Die vorstehenden Betrachtungen und Beispiele zu den verschiedenen risikobeeinflussenden Maßnahmenpaketen unterstreichen die Bedeutung des Begriffs Gefährdung für die risikoorientierte Sicherheitsarbeit im Eisenbahnwesen.

Sie sollten möglichst exakt und auch vollständig erfasst und definiert werden. Dies spiegelt auch die CSM-RA-Verordnung wider, nach der die vom System Eisenbahn ausgehenden Gefährdungen zu identifizieren und in so genannten Gefährdungskatalogen zu führen sind – einschließlich der Maßnahmen zu ihrer Beherrschung. Das Identifizieren von Gefährdungen wie auch das Festlegen und Beschreiben der Maßnahmen, die für die Beherrschung der entsprechenden Risiken erforderlich sind, erfordern die Definition des betrachteten Teils des Systems Eisenbahn einschließlich der umgebenden Randbedingungen. ■

Quellen

1) Bosse, Gunnar. Grundlagen für ein generisches Referenzsystem für die Betriebsverfahren spurgeführter Verkehrssysteme. Dissertation 2011, Online-Veröffentlichung http://www.digibib.tu-bs.de/?docid=00038535
2) Europäische Gemeinschaft. Verordnung (EG) Nr. 352/2009 der Kommission vom 24.04.2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken
3) Europäische Gemeinschaft. Richtlinie über die Eisenbahnsicherheit. Richtlinie 2004/49/EG
4) Eisenbahn-Bundesamt. Leitfaden Anwendung CSM Risikoevaluierung und -bewertung. http://www.eba.bund.de/nn_342570/DE/Infothek/Infrastruktur/Allg__Vorschriften/CSM__Risiko/CSM__Risiko__node.html. Stand 14.10.2013
5) Pachl, Jörn. Glossar der Systemtechnik der Eisenbahn. http://www.joernpachl.de/glossar.htm. Stand 14.10.2013

https://doi.org/10.24355/dbbs.084-202005050938-0